Configurare Controllo file in modo da consentire file protetti da password e altri file non dannosi

Sommario

Introduzione

In questo documento viene descritto come impedire che un file non dannoso venga bloccato dal controllo dei file.

Problema

In alcuni casi, l'attivazione della funzione di "ispezione dei file" blocca i file non dannosi. Questi tipi di file includono:

- File protetti da password
- File dell'applicazione potenzialmente indesiderati (danneggiati)

Questi file sono bloccati da Umbrella perché non possono essere decompressi e scansionati dal nostro strumento antivirus. I file protetti da password possono apparire bloccati sotto la categoria "File protetti". I file danneggiati possono includere file con contenuto crittografato, contenuti archiviati che non possono essere estratti, dati compressi non validi o un'intestazione di archivio non valida oppure file semplicemente compressi o archiviati in un formato non supportato. Anche se questi file possono essere non dannosi, Umbrella li blocca per impostazione predefinita come precauzione, in quanto i file non possono essere digitalizzati.

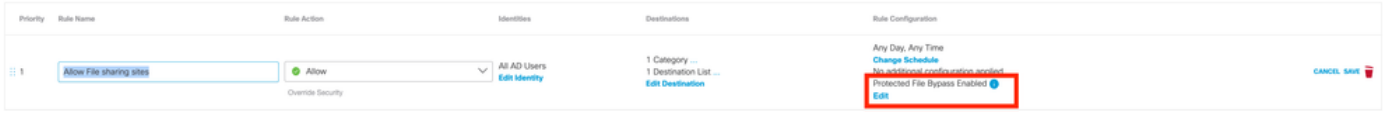
Soluzione

Se si è a conoscenza di un file non dannoso che è stato bloccato a causa di uno dei motivi sopra riportati, è possibile risolvere il problema consentendo l'utilizzo di File protetti. Il comportamento del blocco dei file protetti può ora essere modificato a livello globale o in una singola regola Web.

- Regola (scelta consigliata) - Consenti file protetti per un'identità e/o una destinazione. Eseguire questa operazione se si desidera considerare attendibili i file protetti da una particolare destinazione o ignorare il comportamento per un singolo utente/gruppo.
- Globale: consente di proteggere i file per tutti gli utenti in tutte le regole/set di regole. Effettuare questa operazione se si accetta il rischio di download di file protetti e si preferisce questa opzione al carico amministrativo di creare eccezioni più granulari.

Regola

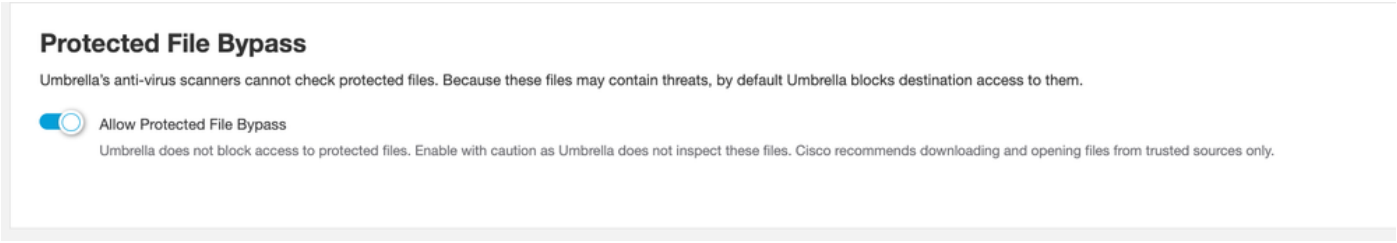
La funzionalità può essere modificata modificando una regola Web nella pagina Criteri > Criteri Web.



10588971481748

Globale

La funzionalità può essere modificata in Criteri > Criteri Web > Impostazioni globali.

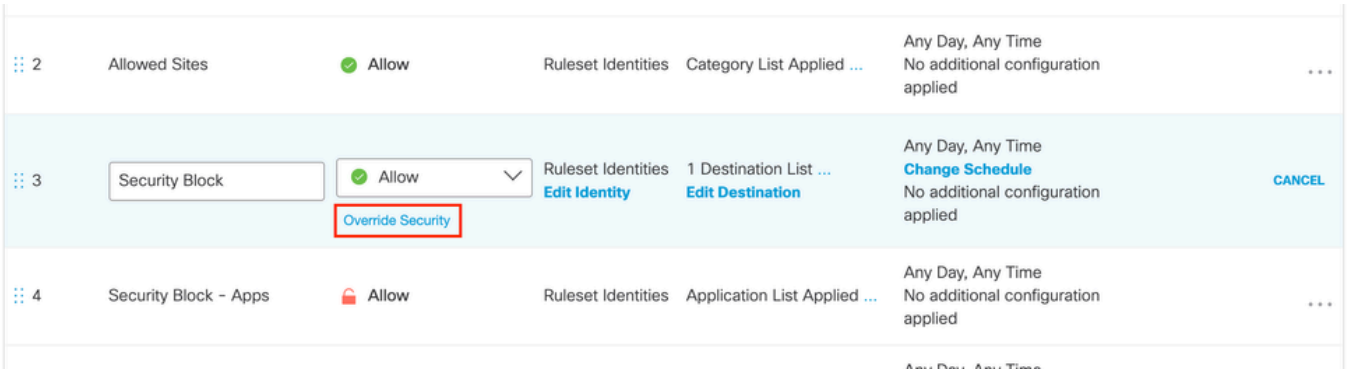


10589018672020

Soluzione alternativa

È inoltre possibile ignorare i problemi relativi all'ispezione dei file utilizzando l'opzione Ignora protezione in qualsiasi criterio Web. Questa opzione deve essere utilizzata con cautela perché disattiva tutte le altre impostazioni di protezione, incluso il blocco di file dannosi.

- Per i file protetti, utilizzare invece una delle soluzioni descritte in questo documento.
- Utilizzare questa opzione solo in circostanze in cui la destinazione è considerata attendibile con assoluta certezza e non si dispone di altre opzioni per risolvere il problema.
- Per i falsi positivi anti-virus, prima di implementare qualsiasi soluzione, verificare che il file sia stato eliminato da Cisco Talos.



Screen_Shot_2021-10-07_at_2.59.04_PM.png

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).